for directing the packet to a cloud service, server, or other device closest to the geo-location data provided in the extension header. For example, device **656** could determine that destination device B **635**, e.g., load balancer is closer to the location of client **605** and, therefore, device **656** could prioritize sending traffic from client **605** to destination device B **635** over destination device A **630**.

[0066] In one embodiment, the present invention provides a method for efficiently routing packets based on the geographic location of the client. This embodiment can, for example, be used in Application Delivery Controllers (ADCs). An ADC is a computer network device in a datacenter, often part of an application delivery network (ADN) that helps perform common tasks such as those done by web sites to remove load from the web servers themselves. Many also provide load balancing. A load balancing device, for example, located in New York, for example, can route packets incoming from California to a different load balancer in California instead of processing it. Or for example, if a client device in California requests a web page of a company with servers in California, the request would be routed to a server in California that is in close proximity

[0067] If providing monitoring services, an in-path device, e.g., device **656** could use the geographic database discussed above to provide location and accuracy trending and tracking data. For example, if device **656** is being used for protection services, feedback regarding the number of requests blocked or limited may be collected and sent to a network administrator. Or, for example, if device **656** is providing service changes, feedback regarding the re-directed traffic could also be transmitted to a network administrator.

[0068] It should be noted that there may be several conceivable applications of the geo-location information inserted into the IPv6 packets in addition to using the geo-location information to authenticate packets, prioritize packets and route packets.

[0069] FIG. **7** depicts a flowchart for an exemplary computer controlled process for managing Internet traffic based on geo-location information in an IPv6 packet in accordance with embodiments of the present invention.

[0070] At step **702**, an IPv6 packet is received by a device in the path of the traffic between a client **605** and a destination device, e.g., device **630** or **635** in FIG. **6**, or by the destination device itself

[0071] At step **704**, the receiving device determines if the IPv6 packet has an extension header with geo-location information.

[0072] Finally, at step **706**, the receiving device makes a decision based on the geo-location information. The decision can, among other things, be related to authenticating, prioritizing or routing the IPv6 packet.

[0073] FIG. **8** depicts a flowchart for an exemplary computer controlled process for authenticating an IPv6 packet based on geo-location information in the packet in accordance with embodiments of the present invention.

[0074] At step **802**, the receiving device analyzes the extension header of the IPv6 packet containing geo-location information.

[0075] At step **804**, the receiving device, determines the geo-location information. As explained above, the geo-location information can, among other things, include latitudinal, longitudinal, and direction information.

[0076] At step **806**, the receiving device determines if the packet is authenticated based on the geo-location information. If the packet is determined to originate from a trusted source, at step **808** it is authenticated and allowed to transmit. If, however, it is determined to originate from an untrustworthy source, at step **810**, the packet is either blocked or flagged for further monitoring.

[0077] FIG. **9** depicts a flowchart for an exemplary computer controlled process for prioritizing an IPv6 packet based on geo-location information in the packet in accordance with embodiments of the present invention.

[0078] At step **902**, the receiving device analyzes the extension header of the IPv6 packet containing geo-location information.

[0079] At step **904**, the receiving device, determines the geo-location information. As explained above, the geo-location information can, among other things, include latitudinal, longitudinal, and direction information.

[0080] At step **906**, the receiving device determines if the packet is to be prioritized based on the geo-location information. As explained above, this determination can be based on relative origin of the IPv6 packet as compared with the location of origin of other IPv6 packets, e.g., prioritizing traffic originating from presenter on stage v/s from a member of the audience. If the packet is determined to need higher priority, at step **908** it is prioritized and allowed to transmit at a higher priority. If, however, it is determined to not require high priority, at step **910**, the packet is routed at regular priority.

[0081] FIG. **10** depicts a flowchart for an exemplary computer controlled process for efficiently routing an IPv6 packet based on geo-location information in the packet in accordance with embodiments of the present invention.

[0082] At step **1002**, the receiving device analyzes the extension header of the IPv6 packet containing geo-location information.

[0083] At step **1004**, the receiving device, determines the geo-location information. As explained above, the geo-location information can, among other things, include latitudinal, longitudinal, and direction information.

[0084] At step **1006**, the receiving device determines if the packet is to be routed differently relative to other packets based on the geo-location information, e.g., packets originating from a given location may be re-routed to servers or load balancers closer to the destination location. If the packet is determined to need special routing, at step **1008** it is routed differently based on a pre-determined policy. If, however, it is determined to require regular routing, at step **1010**, the packet is transmitted regularly without any re-routing.

[0085] While the foregoing disclosure sets forth various embodiments using specific block diagrams, flowcharts, and examples, each block diagram component, flowchart step, operation, and/or component described and/or illustrated herein may be implemented, individually and/or collectively, using a wide range of hardware, software, or firmware (or any combination thereof) configurations. In addition, any disclosure of components contained within other components should be considered as examples because many other architectures can be implemented to achieve the same functionality.

[0086] The process parameters and sequence of steps described and/or illustrated herein are given by way of example only. For example, while the steps illustrated and/or described herein may be shown or discussed in a particular order, these steps do not necessarily need to be performed in the order illustrated or discussed. The various example methods described and/or illustrated herein may also omit one or